Policy - Whistleblower Protection.

Owner: Chief People Officer
Effective date: 27 July 2026
Version: 1.7

Defence Bank Limited ABN 57 087 651 385 | AFSL/Australian Credit Licence 234582

Contents.


ADFA
Defence
Bank

Why this is important.

1. Defence Bank is committed to a culture of legal and ethical behaviour and good corporate governance and creating a workplace environment where employees feel safe to raise concerns of wrongdoing that they have witnessed or reasonably believe has or is occurring.
2. Defence Bank encourages all employees who have concerns about possible wrongdoing or inappropriate behaviour at Defence Bank to raise those concerns in the ordinary course of business. Individuals can do this by contacting their People Leader, the People Team or a Defence Bank Nominated Officer.
3. There may be times when an individual does not feel comfortable speaking up in the ordinary course of business, would like to raise their concerns anonymously, or feel that they need confidentiality and protection. In these circumstances, Defence Bank encourages individuals to raise concerns about wrongdoing in accordance with this policy.
4. This policy is an important tool for helping Defence Bank to identify any wrongdoing that may not be uncovered unless there is a safe and secure means for disclosing it.
5. This policy is underpinned by Defence Bank's principles of being Accountable, Collaborative and Transparent which guide our behaviour and apply to every aspect of our business.

What is the purpose of this policy.

6. The purpose of this policy is to:
   a. encourage genuine concerns about possible wrongdoing in relation to Defence Bank to be raised as soon as possible;
   b. provide guidance in relation to how to raise those concerns, how they will be investigated and the support available to individuals raising concerns under this policy;
   c. ensure that individuals who disclose wrongdoing can do so safely, securely and with confidence that they will be protected and supported; and
   d. ensure that disclosures of wrongdoing that qualify for protection under the law are managed in accordance with the appropriate legislation and this policy.

Who this applies to and when.

7. This Policy applies to everyone at Defence Bank, including all directors, employees, contractors and consultants. It also applies to any person who is in one of the categories of people set out in clause 10.

Definitions.

8. In this Policy:

   APRA means Australian Prudential Regulation Authority.

   ASIC means Australian Securities & Investments Commission.

   ASIC Act means *Australian Securities and Investments Commission Act 2001* (Cth).

   ATO means the Australian Taxation Office.

Corporations Act means *Corporations Act 2001* (Cth).

Detriment has the meaning specified in clause 45.

Eligible Recipient is someone the law recognises as authorised to receive a protected disclosure, as defined in clause 21.

Nominated Officer means a person appointed by the Defence Bank Board of Directors as the preferred recipient of internal disclosures made under this policy. The Nominated Officers are outlined in clause 20.

Protected Report is defined in clause 11.

Taxation Administration Act means *Taxation Administration Act 1953* (Cth).

Whistleblower means a person who falls within one of the categories described in clause 10 of this policy and who makes a report of wrongdoing, based on reasonable grounds, to one of the people described in clause .

Wrongdoing is defined in clause 13 and 14.

Requirements.

What reports are protected under this policy?

9. To be eligible for the legal protections outlined in this policy, an individual must:

   a. be an eligible whistleblower;

   b. have reasonable grounds to suspect wrongdoing in relation to Defence Bank; and

   c. report their concerns to one of the Bank's Nominated Officers, to an Eligible Recipient or to Your Call.

   If their report meets all three of the above these criteria, it is a **Protected Report**.

   If their report doesn't meet the above criteria, we still encourage them to raise their concerns with us. However, only Protected Reports receive the legal protections outlined in this policy.

Who is an Eligible Whistleblower?

10. An eligible whistleblower is defined as any of the following:

    a. an officer or employee of Defence Bank;

    b. a person who supplies goods or services to Defence Bank, whether paid or unpaid, or an employee of such a person;

    c. an associate of Defence Bank;

    d. a spouse, relative or dependent of any of the above; or

    e. someone who was formally any of the above (eg. A former employee).

What must a Whistleblower report be about?

Disclosure to be made with reasonable grounds.

11. To be a Protected Report, a disclosure must be made with reasonable grounds. In practice, this means that there is more than just a suspicion of potential wrongdoing and there is some information that supports the allegation. A Whistleblower does not need to prove the allegations but is encouraged to provide evidence in support of their disclosure if it is safely available.

12. An eligible whistleblower can still qualify for protection even if their Protected Report turns out to be incorrect or unsubstantiated, provided they have a reasonable basis for making the report.

What is wrongdoing?

13. Generally, wrongdoing includes any conduct which an eligible whistleblower has reasonable grounds to suspect:

    a. is about misconduct or an improper state of affairs or circumstances concerning Defence Bank;

    b. is about misconduct or an improper state of affairs or circumstances in relation to the tax affairs of Defence Bank or an associated company which the eligible whistleblower considers may assist to perform the functions or duties in relation to the tax affairs of Defence Bank;

    c. indicates that Defence Bank or any of its officers or employees has engaged in conduct that:

        i. involves a breach of or is an offence against any of the following Commonwealth laws: the *Corporations Act 2001*, the *ASIC Act 2001*, the *Banking Act 1959*, the *Financial Sector (Collection of Data) Act 2001*, or the *National Consumer Credit Protection Act 2009,* or regulations made under those laws;

        ii. is an offence against any other Commonwealth law that is punishable by imprisonment of 12 months or more;

        iii. indicates a systemic issue that a relevant regulator (e.g. ASIC or APRA) should know about to properly perform its functions;

        iv. indicates a significant risk to public safety or the stability of, or confidence in, the financial system, even if it does not involve breach of a particular law; or

        v. is indicative of dishonest or unethical behaviour or practices that may cause consumer harm.

    These matters are referred to as '**wrongdoing**' in this policy.

Examples of conduct that may be reported as wrongdoing.

14. Examples of the types of matters that may be reportable as wrongdoing include, but are not limited to:

    a. Fraud (including dishonest activity, deliberate falsification, knowingly publishing or providing documentation that is false, misappropriation of funds, covering up fraud);

b. Corrupt behaviour (including bribery, dishonestly failing to act or dishonestly taking advantage of an employment position);

c. Conduct leading to unfair customer outcomes;

d. Misconduct or unethical behaviour (including discrimination, sexual harassment and serious breaches of Defence Bank's Code of Conduct and workplace policies);

e. Legal or regulatory non-compliance (including breaches of financial services laws, Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF) laws, Modern Slavery laws);

f. Illegal conduct, such as theft, dealing in, or use of illicit drugs, violence or threatened violence, and criminal damage against property;

g. Unsafe work practices or not properly responding to a serious safety issue;

h. Serious inappropriate or unethical conduct such as gross mismanagement, serious and substantial waste of company resources or repeated breaches of administrative procedures;

i. Taking or threatening to take detrimental action against a person who has made a disclosure or is suspected to have made, or planning to make a disclosure;

j. Deliberate concealment of information relating to any of the matters listed above.

Generally, wrongdoing does not include personal work-related grievances. See clause 16-17.

False reporting.

15. False reporting will be treated seriously. If we find that a Whistleblower has intentionally made a false report (for example, if they know a report is untrue and they report it to harm, annoy, or cause distress to someone), the Bank may take disciplinary action against the individual/s in accordance with other Defence Bank policies and procedures.

What should I do if I have a personal work-related grievance?

16. We encourage everyone to speak up about concerns. However, reports that relate solely to personal work-related grievances are not generally considered to be wrongdoing and are therefore not covered by this policy. Personal work-related grievances should be internally raised using the Grievance policy.

17. Personal work-related grievances typically relate to an individual's current or former employment arrangements, performance, remuneration outcomes or personal circumstances that do not have significant implications for the organisation (for example an interpersonal conflict between an individual and another employee, or a decision about an individual's employment that does not breach workplace laws).

18. In some circumstances, a grievance may be a protected report, refer Appendix 2 for more guidance.

Who can receive a disclosure?

19. To qualify for protection as a whistleblower, the disclosure must be made to an Eligible Recipient. While a disclosure can be made to any Eligible Recipients, Defence Bank has appointed four Nominated Officers to receive disclosures in the first instance.

20. Our Nominated Officers are:

    a. Chief People Officer;

    b. Chief Risk Officer;

    c. Chief Financial Officer; and

    d. Company Secretary.

21. In addition, other Eligible Recipients authorised to receive a protected report include:

    a. A Director or Executive of Defence Bank;

    b. Regulatory bodies, for example: ASIC, APRA, or a prescribed Commonwealth authority; or

    c. Defence Bank's auditors or a member of an audit team conducting an audit of Defence Bank.

22. A protected disclosure can also be made to Your Call, our external, independent whistleblower service.

    a. Online: https://www.yourcall.com.au/report - enter Defence Bank's unique identifier code DEF833205.

    b. By phone using Your Call's external reporting hotline: 1300 790 228 (9am to midnight AEST on business days).

    c. If an individual has a hearing or speech impairment, they can contact Your Call online or they can contact Your Call by phone, via the National Relay Service. Simply choose your contact method at www.accesshub.gov.au and request Your Call's hotline 1300 790 228.

23. Disclosures made to a legal practitioner, for the purposes of obtaining legal advice or representation in relation to the operation of the whistleblower provisions in the Corporations Act, are protected.

24. Disclosures can be made to a journalist or a parliamentarian, in certain circumstances. A public interest or emergency disclosure can be made; however, it must be in the form of a written notice which has previously been made to ASIC, APRA, or a prescribed body, at least 90 days before that time. The whistleblower should seek independent legal advice before making a public interest or emergency disclosure. Refer Appendix 1 for further guidance.

How to make a disclosure.

25. Disclosures can be made in person, in writing (ie. in email or the online submission form), or by telephone.

26. Disclosures may be made anonymously, securely and both within and outside business hours.

What to include in a disclosure.

27. Defence Bank encourages a whistleblower making a disclosure to provide as much detail as possible and provide supporting evidence if appropriate. This should include:

    a. Dates, times, and locations of the suspected wrongdoing;

    b. Names of any people involved;

    c. The nature of the concern;

    d. How you became aware of the issue;

    e. Any witnesses to the conduct being raised;

    f. Any concerns about detriment because of making the disclosure; and

    g. Any other information that may support the disclosure.

Can I remain anonymous when making a report?

28. A whistleblower can remain anonymous when making a Protected Report. There is no requirement to provide an individual to name or identify themself at any stage during the reporting or investigation process or after the investigation is finalised. They can also decide not to answer questions that they feel may reveal their identity.

29. They can also choose to provide their identity to the person that they are making the report to but not consent to them sharing their identity with anyone else.

Communication with a discloser.

30. Defence Bank encourages disclosers who would prefer to remain anonymous to maintain ongoing two-way communication with Defence Bank so they can be asked any follow up questions and be provided feedback from the investigation.

31. The Your Call message board is the default way that Defence Bank will communicate with anonymous reporters. This enables:

    a. Communication between Your Call and Defence Bank without revealing the discloser's identity;

    b. A discloser to securely upload any relevant documentation and/or material;

    c. Two way communication between Defence Bank and the discloser; and

    d. The ability to request support or report detriment.

    e. Employees may also contact our Employee Assistance Program: Uprise.

Nominated Officer responsibilities.

32. Nominated Officers are the preferred point of contact for making a Protected Report and are responsible for:

    a. assessing and triaging disclosures;

    b. overseeing investigations;

    c. ensuring appropriate escalation and reporting; and

d. safeguarding the confidentiality and protection of Whistleblowers.

Disclosures made to other Eligible Recipients.

33. An Eligible Recipient who is not a Nominated Officer may still receive a Protected Report. Where this occurs, the Eligible Recipient must:

a. maintain the confidentiality of the disclosure and the identity of the whistleblower;

b. not disclose information that may identify the whistleblower unless permitted by law;

c. not cause, or threaten to cause, detriment to the whistleblower; and

d. promptly refer the disclosure to a Nominated Officer so it can be managed in accordance with this Policy.

Protection available to Whistleblowers.

34. If a whistleblower makes a Protected Report, they are entitled to the benefit of certain protections in accordance with the *Corporations Act* or the *Taxation Administration Act*. These protections apply regardless of whether they make a Protected Report to one of our Nominated Officers, to Your Call or to another Eligible Recipient in accordance with this policy.

Protecting the Whistleblower's identity.

35. If a whistleblower makes a Protected Report, their disclosure will be treated as confidential in accordance with legal requirements.

36. If a whistleblower makes a Protected Report, it is illegal for a person to disclose their identity or information that is likely to lead to identification of their identity, except where permitted or required by law.

37. Defence Bank will only disclose the whistleblower's identity:

a. to ASIC, APRA, or a member of the Australian Federal Police;

b. to a professional legal advisor (including Defence Bank's legal team) for the purpose of obtaining legal advice or representation; or

c. with the consent of the whistleblower.

38. Defence Bank may disclose information that is reasonably necessary for the purposes of investigating the report, provided that the information does not include the whistleblower's identity. All reasonable steps will be taken to reduce the risk that the whistleblower will be identified from the information contained within the disclosure and any supporting documentation.

39. To maintain confidentiality of a whistleblower's identity, Defence Bank will:

a. ensure personal information or references to the whistleblower's identity is redacted in all investigation and reporting documents;

b. refer to the whistleblower in gender-neutral terms;

c. where possible, contact the whistleblower to help identify certain aspects of their disclosure that could inadvertently identify them;

d. ensure that the information a whistleblower provides and all materials relevant to a Protected Report are held securely with access limited only to the individuals necessary to investigate the Protected Report, and to support and protect the Whistleblower; and

e. take reasonable steps to ensure its personnel understand the requirements of this policy.

40. A whistleblower should also be aware that during an investigation, it may be necessary for Defence Bank to tell the people who are believed to be involved in the wrongdoing about the alleged wrongdoing. This is to ensure a fair investigation and provide those people with an opportunity to respond to the allegations. Although the Bank will not tell these people the Whistleblower's identity unless they give consent, it is possible that the details of the report may lead them to believe that they know the identity of the Whistleblower.

41. Any breach of confidentiality will be treated as a serious matter and may be the subject of disciplinary action. Breaches of Whistleblower confidentiality are also an offence under the *Corporations Act* and the *Taxation Administration Act* and serious penalties apply for both individuals and corporations.

42. If a Whistleblower believe their confidentiality as a Whistleblower has been breached, they can lodge a complaint with either a Nominated Officer, any Eligible Recipient, Your Call or directly with ASIC, APRA or the ATO.

Protection against detrimental conduct.

43. Defence Bank is committed to protecting the rights of Whistleblowers who have made Protected Reports and will not tolerate any detriment or threats of detriment against them or any other person (e.g. suspected whistleblowers or people who participate in investigations).

44. It is an offence under the *Corporations Act* and the *Taxation Administration Act* to cause, or threaten to cause, detriment to a person because they or someone else has made, may have made, proposes to make or could make a Protected Report and serious penalties apply for both individuals and corporations.

45. Examples of detrimental conduct that is prohibited under the law includes, but is not limited to:

a. Dismissal of an employee;

b. Suspension of an employee;

c. Alternation of an employee's position to their disadvantage;

d. Discrimination, harassment, intimidation or victimisation of a person;

e. Harm or injury to a person including psychological harm;

f. damage to property;

g. damage to reputation;

h. damage to business or financial position;

i. victimisation in external or internal communications; or

j. any other damage.

46. The following actions are not considered to be detriment:

a. reasonable administrative action taken to protect a Whistleblower from detriment (e.g. relocating them to another office to prevent them from detriment);

b. managing the unsatisfactory work performance of a Whistleblower, in line with Defence Bank's usual performance management framework;

47. Defence Bank will protect Whistleblowers from detriment arising from making a Protected Report by undertaking the following measures:

    a. conducting an assessment of the disclosure to manage the risk of detriment to the Whistleblower;

    b. make reasonable adjustments as required to allow the Whistleblower to perform their duties at work without being potentially exposed to detriment (e.g. by changing reporting lines or location);

    c. implement strategies to help the Whistleblower minimise and manage stress, time or performance impacts or other challenges resulting from the disclosure or its investigation;

    d. make available support services such as access to Defence Bank's independent Employee Assistance Program (EAP);

    e. Ensure management are aware of their responsibilities to maintain the confidentiality of a disclosure, address risks of harassment or isolation, manage other conflicts and fairness relating to the whistleblower; and

    f. Implement interventions for protecting the Whistleblower if detriment has already occurred (in line with the investigation section of this policy).

48. An eligible whistleblower who is subject to detriment may seek compensation or other remedies from a Court if they have suffered loss, damage or injury because of a Protected Report or because Defence Bank failed to take reasonable precautions and exercise due diligence to prevent the detriment.

49. The whistleblower may choose to see independent legal advice in relation to their rights if they believe they have suffered detriment. They can also advise one of the bank's Nominated Officers, contact Your Call or contact ASIC, APRA or the ATO.

Protection for Whistleblowers against litigation.

50. If a Whistleblower makes a Protected Report, they are protected from any of the following legal actions for doing so:

    a. Civil liability (e.g. any legal action against an individual for breaching an employment contract, a duty of confidentiality or another contractual obligation);

    b. Criminal liability (e.g. legal action against an individual for unlawfully releasing information, or other use of the Protected Report against them in a criminal proceeding (other than for making a false disclosure);

    c. Administrative liability (e.g. disciplinary action for making the Protected Report).

51. These protections do not grant immunity for any misconduct an Eligible Whistleblower has engaged in, that is revealed through their disclosure.

Support available for Whistleblowers.

52. Defence Bank will support anyone who has made a disclosure and will protect Eligible Whistleblowers from detriment.

53. If necessary, Defence Bank will appoint a Protection Officer to arrange or coordinate support and protection for Whistleblowers who have made or are in the process of making a Protected Report. A Whistleblower can contact any of the Nominated Officers to discuss how a Protection Officer may be able to provide support and protection.

54. The role of the Protection Officer is to:

    a. assess the immediate welfare and protection needs of a Whistleblower;

    b. safeguard the interests of a Whistleblower in accordance with this policy and the law; and

    c. address any issues or concerns of detriment.

How we handle and investigate Protected Reports.

55. Any person who receives a Whistleblower report made under this policy must ensure that the report is managed in compliance with this policy and any relevant procedures. This is to ensure that the protections available for the Whistleblower are not compromised and that Defence Bank meets its legal obligations.

56. Where a report is made to Your Call, they will provide Defence Bank's Nominated Officers with a copy of the disclosure and any relevant supporting documents.

57. If a report relates to a particular Nominated Officer, that Nominated Officer is excluded from all communications in relation to the receipt and investigation of disclosure report.

58. If a report relates to an Executive Leader, Nominated Officer or a Defence Bank Director, the Risk & Compliance Committee (RCC) would provide oversight of the investigation to ensure if it timely, independent and effective. If the report relates to a Director who is a member of RCC, oversight would be provided by the Chair of the Board. If a report relates to the Chair of the Board, oversight would be provided by either the Chair of RCC or Chair of the Governance & Remuneration Committee.

How do we investigate reports of wrongdoing?

59. Reports of alleged wrongdoing made in accordance with this policy will be treated seriously and where appropriate will be thoroughly investigated by Defence Bank in accordance with this policy.

60. After receiving a report about wrongdoing, we will assess the information provided to determine whether it is a Protected Report, how it will be handled and whether an investigation is required. The precise steps to be taken to investigate a report will differ in individual cases but may include:

    a. determination of the nature and scope of an investigation;

    b. appointment of an internal or external investigator (if it has been determined that an investigation is required) who is able to conduct the investigation in a fair, objective and independent manner;

c. the investigator or other person asking the Whistleblower whether they consent to their identity being disclosed to investigate the report;

d. interviewing the Whistleblower and any other relevant person to obtain information about the report;

e. determination of the nature of any technical, financial or legal advice that may be required to support the investigation;

f. review of relevant documents and other information in relation to the report;

g. the investigator making findings regarding the conduct reported.

61. Generally, if the Whistleblower can be contacted, we will confirm receipt of their disclosure within two business days. The investigation of a Protected Report will commence as soon as reasonably possible from the date we receive it. However, there may be reasons why an investigation may take longer. If we think there might be a delay with the investigation, we will tell the person who made the Protected Report (where possible).

62. Where possible and assuming that the identity of the Whistleblower is known, the Whistleblower will be kept informed of when the investigation process has begun, while the investigation is in progress and after the investigation has been finalised, subject to confidentiality and privacy considerations. Where a reporter is anonymous, communications will be via the Your Call online message board.

Treatment of employees who are the subject of a Whistleblower report.

63. Defence Bank will take all reasonable steps to ensure that any employee who is the subject of a Protected Report is afforded fair treatment and an impartial investigation in accordance with this policy. Generally, when an investigation is conducted, employees who are the subject of a Protected Report may be, within the constraints of confidentiality:

a. told about the substance of the allegations;

b. given a fair and reasonable opportunity to respond to the allegations before the investigation is finalised; and

c. informed about the findings of the investigation and given an opportunity to respond to those conclusions before any action is taken against them (subject to legal, privacy and confidentiality requirements).

64. Before providing any information to an employee who is the subject of a Protected Report we will:

a. make sure the information does not include the whistleblower's identity;

b. make sure we have taken all reasonable steps to reduce the risk that the whistleblower will be identified from the information; and

c. only provide information that is reasonably necessary for investigating the issues raised in the Protected Report.

65. Employees who are the subject of a Protected Report may access Defence Bank's independent Employee Assistance Program (EAP) for additional support.

Decision outcomes.

66. Decisions about investigation, employment outcomes, and whistleblower protection measures will be made by separate individuals where practicable (and documented).

67. Defence Bank may decide to take action in response to any findings which may include, but is not limited to, disciplinary action, reporting the matter to an appropriate regulator, conducting training or addressing procedural and policy deficiencies.

Internal reviews.

68. If Whistleblower makes a Protected Report, or an individual is the subject of a Protected Report, and they are not satisfied with the outcome, they may ask for an internal review of the Bank's decision.

69. Internal reviews will be directed to the CEO or Chair of the Board, or an alternative Nominated Officer if there is a conflict.

70. The Bank may refuse to conduct an internal review if no new information is available or if the new information would not change the outcome.

71. If the Whistleblower is not satisfied with the Bank's response, they may lodge a report or complaint with ASIC, APRA or the ATO in accordance with the law.

Reporting to the Board.

72. The Board (through the Risk and Compliance Committee) will be provided with a confidential report on the number and type of whistleblowing incidents quarterly to enable it to address any issues at a regional or group level. Reports will be on a 'no names' basis to maintain the confidentiality of matters raised under this policy.

73. The Board will monitor the whistleblower management system to ensure that the broader trends, themes and/or emerging risks highlighted by the disclosures made under this policy are addressed and mitigated as part of Defence Bank's risk management and corporate governance.

74. The Board are responsible for appointing and approving the Bank's Nominated Officers.

Review, Access and Training in relation to this policy.

75. This policy will be available to officers and employees of Defence Bank on the intranet. A copy will also be available on our website to ensure it is accessible for all eligible whistleblowers.

76. This policy may be reviewed and amended from time to time and will be reviewed by Defence Bank at least every three years.

77. The Chief People Officer will be responsible for ensuring upfront and ongoing education and annual training on the whistleblower policy, processes and procedures to all officers and employees.

Roles and responsibilities.

78. The roles and responsibilities under this Policy are set out in the table below:

Position.	Responsibilities.
Board **(Policy approver)**	Approve the Whistleblower Policy and any material changes, ensuring it meets legal and governance requirements. Appoint and approve the Nominated Officers (preferred internal recipients) and periodically review their suitability. Oversee the effectiveness of the whistleblower program via regular reports (through the Risk & Compliance Committee), monitoring disclosure trends, emerging risks, and key metrics (e.g. investigation timeliness, outcomes, actions taken) Ensure that systemic issues or themes identified through disclosures are addressed within the broader risk management and corporate governance framework If appropriate, advising the Document Owner to make any amendments that the Board thinks are necessary.
Risk & Compliance Committee (RCC)	Review quarterly whistleblower reports (de-identified) on disclosures, including details of cases, outcomes, and thematic insights. Monitor management's handling of whistleblower matters, ensuring investigations are timely, independent, and effective. Advise the Board on program improvements or resource needs to strengthen Defence Bank's whistleblower framework.
Chief People Officer **(Policy Owner and Key Contact)**	Maintain policy compliance with legal requirements (Corporations Act, Taxation Admin Act, APRA standards) and ensuring alignment with ASIC's RG270. Review and update the policy at least triennially (or earlier if regulatory changes occur) and recommend non-material changes where needed. Ensure organisation-wide training (initial and annual refreshers) on whistleblowing procedures and protections. Provide assurance to the Board (at least annually) that the whistleblower program is effective, including policy adequacy, training completion rates, and any improvement plans. Helping the Chief Executive Officer (CEO) and the Board meet their responsibilities by interpreting the Policy, providing training and expert advice, and answering questions about the Policy. Oversight of Whistleblowing Program.
Nominated Officers	Receive and assess whistleblower disclosures. Determine triage, investigation approach and escalation. Safeguard Whistleblower confidentiality and manage conflicts of interest. Oversee investigations by appointing an appropriate Whistleblower Investigations Officer.

Position.	Responsibilities.
	Support and protect the Whistleblower. Report and escalate material matters to the CEO and Board as appropriate.
Eligible Recipients	Accept whistleblower disclosures and treat them with strict confidentiality. Immediately escalate the disclosure to a Nominated Officer (or via Your Call) for formal management under this Policy. Facilitate the protected channel by connecting the Whistleblower with a Nominated Officer. Fulfil legal duties: do not reveal the Whistleblower's identity or cause detriment; recognize personal liability for breaches if disclosures are mismanaged.
Employees and contractors	Complying with this Policy and being guided by it. Do not engage in any conduct that causes harm or disadvantage to a Whistleblower because they have made, are considering making, or as a consequence of making, a Protected Report.
Managers	Ensuring that employees are aware of this policy and how to report wrongdoing. Do not engage in any conduct that causes harm or disadvantage to a Whistleblower because they have made, are considering making, or as a consequence of making, a Protected Report.
Whistleblower Investigation Officer (WIO) *(Appointed by a Nominated Officer to investigate a disclosure)*	Lead or coordinate investigations into disclosures, following best practices for fairness, impartiality, and thoroughness. Maintain confidentiality and ensure no unauthorised sharing of information occurs during investigations. Report investigation findings and recommendations to the relevant Nominated Officer for decisions on outcomes and further actions. Note: The WIO may be an internal role (where independent) or an external investigator engaged for specific cases.
Whistleblower Protection Officer (WPO) *(Appointed by a Nominated Officer on a case-by-case basis; typically, an independent senior leader, e.g. the CRO)*	Assess and manage detriment risk to the Whistleblower from the point of disclosure throughout the investigation.- Implement and coordinate support measures for the Whistleblower (e.g., changes to working arrangements, provision of counselling services) Monitor and intervene if any signs of retaliation or adverse treatment arise, ensuring timely action to prevent or mitigate detriment. Appointed by a Nominated Officer if requested by a Whistleblower. Work with the Whistleblower to understand and manage welfare concerns arising from making a Protected Report, and help support a supportive work environment. This is normally the Chief Risk Officer.

Breaches.

79. If this Policy is breached, Defence Bank may take disciplinary action. This will depend on the circumstances, including if the breach is deliberate, how severe it is and if there have been previous occurrences. Disciplinary action could include a warning, dismissal, or Defence Bank ending its business relationship.

80. If the law is broken, an individual might face criminal or civil liability.

81. Breaches of this Policy should be reported to a Nominated Officer or to Your Call directly.

Contacts for questions and more information.

This Policy is owned by the Chief People Officer. If you have any questions or would like more information about this Policy, you should contact the Chief People Officer.

Document information.

Effective from	27 July 2026
Owner	Chief People Officer
Approver	Board
Next review due	July 2029
Entities this applies to	Defence Bank Limited, its subsidiaries and any other entity or joint venture which it controls (collectively **Defence Bank**) except those which have been given exemption as shown below.
Exemptions	N/A
Related documents	Key documents that should be read in conjunction with this Policy: • People Operational Policy; • Defence Bank Process - Speak Up reporting process; • *Corporations Act 2001* (Cth); • *Taxation Administration Act 1953*; and • ASIC Regulatory Guide 270 - Whistleblower policies.

Document history.

Version.	Date.	Amended by.	Details of amendment.
1.0.	24/07/2023	Chief People Officer	New standalone policy to replace Policy 8, section 3.
1.1	17/10/2023	Chief People Officer	Review cycle updated from 2 to 3 years. And CDIO update to CTDO.
1.2	31/10/2023	Chief People Officer	All clause cross references updated as they were incorrect.
1.3	21/11/2023	Chief People Officer	Clause 11.c.i updated to reflect correct year.
1.4	30/06/2024	Chief People Officer	Clause 12.e updated to add Modern Slavery

Version.	Date.	Amended by.	Details of amendment.
1.5	26/02/2026	Chief People Officer	Clause 16 updated with new link and Appendix 1 position titles updated.
1.6	31/03/2026	Chief People Officer	Details of Nominated Officer updated from M.Simos to A.Cox.
1.7	27/07/2026	Chief People Officer	Triennial review. Complete review and rewrite of entire policy to ensure accessibility. Converted to third person references instead of second person.

Appendix 1.

Public interest and emergency disclosures.

The whistleblower should seek independent legal advice before making a public interest disclosure or an emergency disclosure.

Public interest disclosures.

A whistleblower may make a disclosure in the public interest to a member of parliament or a journalist if:

- they have previously made that disclosure to ASIC, APRA or another Commonwealth body prescribed by regulation; and
- at least 90 days have passed since the disclosure was made and they do not have reasonable grounds to believe that action is being, or has been, taken to address the misconduct to which the previous disclosure related; and
- They have reasonable grounds to believe that making a further disclosure of the misconduct would be in the public interest; and
- after the end of the 90-day period they notify the body to whom you made the disclosure (ASIC, APRA or other Commonwealth body) in writing with sufficient information to identify the previous disclosure, and state that they intend to make a public interest disclosure to a member of parliament or a journalist; and
- the extent of the information disclosed in the public interest disclosure is no greater than is necessary to inform the recipient of the misconduct or the improper state of affairs or circumstances.

Emergency disclosures.

A whistleblower may make an emergency disclosure to a member of parliament or a journalist if:

- they previously made that disclosure to ASIC, APRA or another Commonwealth body prescribed by regulation;
- they have reasonable grounds to believe that the information concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment;
- they notify the body to whom you made the disclosure (ASIC, APRA or other Commonwealth body) in writing with sufficient information to identify the previous disclosure, and state that they intend to make an emergency disclosure to a member of parliament or a journalist;
- the extent of the information disclosed in the emergency disclosure is no greater than is necessary to inform the recipient of the substantial and imminent danger.

It is important to understand that a report may only be made to a journalist or a parliamentarian in the circumstances described above.

Appendix 2.

Personal work-related grievances.

Clause 13 sets out what can be reported as wrongdoing under this policy and in accordance with Australian whistleblowing protection laws. In some circumstances, a personal work-related grievance may be a protected disclosure if, in summary:

- it includes information about wrongdoing or information about a personal work-related grievance or is bundled with a report of wrongdoing (mixed report);
- it relates to a breach by Defence Bank of employment or other specified laws punishable by imprisonment of 12 months or more;
- it includes information about wrongdoing beyond an individual's personal circumstances, demonstrates a systemic issue within Defence Bank, has significant implications for Defence Bank or indicates that Defence Bank has engaged in conduct that represents a danger to the public;
- concerns detriment to a person because they have or may be considering reporting wrongdoing; or
- it is made to a legal practitioner for the purposes of obtaining advice or legal representation in relation to the operation of the law about whistleblowers.